ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.19, No.10, October 2008, pp.2628−2637
DOI: 10.3724/SP.J.1001.2008.02628

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

ServLoc:无线传感反应网络的安全位置服务机制*

马建庆+, 钟亦平, 张世永

(复旦大学 计算机与信息技术系,上海 200433)

ServLoc: Secure Location Service for Wireless Sensor and Actuator Network

MA Jian-Qing+, ZHONG Yi-Ping, ZHANG Shi-Yong

(Department of Computing and Information Technology, Fudan University, Shanghai 200433, China)

+ Corresponding author: E-mail: jqma_edu@yahoo.com.cn

Ma JQ, Zhong YP, Zhang SY. ServLoc: Secure location service for wireless sensor and actuator network. *Journal of Software*, 2008,19(10):2628−2637. http://www.jos.org.cn/1000-9825/19/2628.htm

Abstract: To solve the problem of secure location service, this paper proposes a range-free secure localization protocol—ServLoc localization protocol. By means of authenticating messages, hidden actors passively receiving localization requests and filtering false location reports, etc, ServLoc localization protocol can defend location attacks, keep location in privacy and locate sensor node in a distributive way. In addition, this paper also proposes a voting-based location verification scheme—ServLoc verification protocol and ways to defend actor attacks. The analysis illustrates that ServLoc verification protocol can trade off the security and effective localization problem of WSAN. ServLoc scheme can also effectively provide secure location service, even if the WSANs suffer location attacks.

Key words: wireless sensor network; wireless sensor and actuator network; secure location service; localization

摘 要: 为解决无线传感反应网络的安全位置服务问题,提出了一种距离无关的安全定位协议——ServLoc 定位协议.在该协议中,反应器通过认证消息包、被动接收定位请求、过滤虚假信息等方法进行位置攻击防御,位置匿名和分布地确定传感器节点位置.另外也提出了一种基于表决的位置校验协议——ServLoc 校验协议,并对反应器攻击的防御方法进行了初步探讨.分析说明,该协议能够有效地平衡位置欺骗攻击的成功率和定位失效率,并在网络遭受位置攻击时,仍能有效地完成安全位置服务.

关键词: 无线传感器网络;无线传感反应网络;安全位置服务;定位

中图法分类号: TP393 **文献标识码**: A

无线传感反应网络(wireless sensor and actuator network,简称 WSAN)是传感器网络的一种衍生物.它由大量的传感器、一定数量的反应器和基站组成,通过无线介质,协作完成分布感应和反应任务.相对传感器而言,反应器有较充足的资源,其主要功能是处理本地区域传感器感应数据,并分布地对事件做出适当的反应.无线传感反应网络在军用和民用领域都有着广阔的应用前景.例如,在森林防火中,传感器节点感应到火苗,立刻通知本

* Supported by the National Natural Science Foundation of China under Grant No.60672113 (国家自然科学基金); the National Basic Research Program of China under Grant No.2005CB321906 (国家重点基础研究发展计划(973))

Received 2007-03-27; Accepted 2007-06-30

地的反应器(喷水器)进行喷水灭火,防止星火进入不可控制的森林大火状态;在战场上,当传感器节点感应到众多敌人进入某个区域时,特定的反应器(如地雷、鱼雷、导弹)根据预先设定的需求进行集中打击;在抢险救灾中,传感器发现幸存者,然后和附近分布的机器人(反应器)协调救人.可以推断,类似这样的无线传感反应网络将在未来得到更为广泛的应用[1,2].

对节点的有效定位是无线自组织网络的基本功能之一,对网络的应用有效性起着关键的作用.在无线传感器网络中,大多数定位系统使用锚节点(锚节点通过 GPS 或人工配置等手段获取物理位置)协助定位未知节点,一般分两个阶段:1) 测量未知节点到附近锚节点的距离;2) 通过这些第 1 阶段获得的参考距离,利用数学方法对未知节点的位置进行计算.在第 1 阶段中,定位系统通常通过衡量接收信号强度指示 RSSI(received signal strength indication)[3],信号到达时间差 TDOA(time difference of arrival)[4]或跳数[5]等方法进行距离估算;第 2 阶段中采用三边测量法、三角测量法或极大似然估计法等进行位置确定[2,6].这些机制大多需要额外的定位基础设施,如 GPS、超声波、方向天线等,从而提高了网络部署成本,而且不能保证定位的安全性和重要节点位置的隐匿性.

当无线传感反应网络部署在未保护或敌对环境中时,攻击者可能捕获并篡改传感器/反应器内置程序或仿冒网络传感器节点,进行虚报感应信息或位置信息,引诱反应器进行无效的反应活动,破坏网络的正常运行功能.另外,如果攻击者能够检测到节点的物理位置,就可能发动各种攻击,破坏重要节点.虽然安全定位能够用所有传感器节点部署安全 GPS 或人工配置实现,但出于成本或网络扩展性考虑,采用 GPS 和人工配置所有传感器节点进行定位,并不适合大规模无线传感反应网络的部署[6].

已有的传感网络安全定位机制如文献[7−10]等,并不十分适合无线传感器反应器网络部署,主要有下述 3 个原因:1) 与传感器网络不同,传感反应网络中分布的反应器位置已知,可作为锚节点对未知传感器节点进行定位,以节省部署成本,提高网络部署的方便性;2) 鉴于节点的异构性即反应器拥有相对充裕的资源,未知传感器节点的定位计算也可以通过反应器节点协调完成,以节省传感器节点能量等资源开销和提高定位安全性等;3) 反应器是传感反应网络中的重要节点,也是攻击者的重点攻击对象,因此,必须保证反应器在参与定位的同时,保证自身位置的隐匿性和安全性,防止物理捕获或破坏.另外,就我们所知,国内外目前还没有针对无线传感反应器网络的安全位置服务机制进行研究.

本文首先概括了无线传感反应网络中的各类位置攻击模型,分析了实现安全位置服务可以利用的无线传感反应网络特征.并据此提出了一种经济的、自组织的、低能耗和安全的位置服务机制——ServLoc.ServLoc 的定位机制无需额外的定位基础设施,其基本思想是,通过反应器分布协调、隐藏和移动反应器位置、被动接收定位请求来协助传感器节点定位和反应器位置隐匿.ServLoc 定位协议采用了错误或欺骗信息过滤机制和迭代求精方法,提高了定位的精确性和鲁棒性.在 ServLoc 的位置校验机制中,由于采用投票表决机制和误差容忍机制,即使是在网络中存在一定强度的位置攻击和参考距离估算误差的情况下,ServLoc 机制仍能对传感器节点进行有效的安全定位.另外,本文也阐述了对传感器每跳距离的估算方法,以提高定位的精确性.

1 网络模型

安全位置服务包括安全定位、位置校验、位置隐匿和安全位置报告.本文的主要目标就是解决适合无线传感反应网络中的安全位置服务问题,并具有鲁棒性,即在各类位置攻击存在的情况下,ServLoc 仍能提供有效的安全位置服务.

1.1 安全定位服务的攻击模型

我们假设无线传感反应网络中的反应器位置信息已知,而传感器节点需要被定位.这样可以把无线传感反应网络的位置攻击模型分为 3 类:传感器攻击、反应器攻击和外来节点攻击.传感器攻击是仿冒或被捕获的传感器节点通过欺骗定位系统,提供给被定位节点虚假位置信息;反应器攻击是恶意反应器节点通过欺骗其他定位反应器或未知传感器节点,达到传感器节点定位错误;外来节点攻击是外来节点通过信号阻塞、改变信号强度等手段扰乱定位系统的定位精度或使定位失效.几乎所有的基于 TOA,TDOA,AoA,DV-Hop 等的定位机制都

容易受到这些攻击.例如,在传感器攻击中,被捕获的传感器节点通过修改跳数使得定位第 1 阶段中的距离估算错误,进而使得这些基于 DV-Hop 机制的定位系统错误或失效;反应器攻击中,反应器节点作为锚节点可能虚报自身节点位置或直接修改参考距离等手段来扰乱定位机制;在外来节点攻击中,攻击者在锚节点和未知节点间设置信号吸收壁,改变信号强度,使得这些基于信号强度估算距离的定位系统失效.

1.2 ServLoc安全位置服务的特点

与传感器网络安全位置服务机制不同,ServLoc 主要根据无线传感反应网络的特性而提出,具有以下 3 个主要特点:

1) 反应器位置已知,相对于传感器节点,属于稀疏分布,通信范围大.因此,反应器作为锚节点协助定位时,不能采用基于距离的定位机制.ServLoc 协议采用类似 DV-Hop 机制[5],本地区域内的反应器作为锚节点,对未知传感器节点进行定位,避免了采取基于距离的定位机制时,必须增加锚节点而造成网络部署成本的增加.

2) 反应器节点可能是重要节点,必须提供位置隐匿性.因此,当它们充当锚节点时,不能主动发送信标信号而暴露位置信息.但是,反应器相对传感器有较少的资源限制,因此可用作定位中的距离计算和传感器位置计算,以节省传感器能量,均衡网络能量消耗.ServLoc 主要利用反应器节点的协调、迭代计算、错误/误差信息过滤、投票表决等方法给出了未知传感器节点的位置信息,不但能够均衡网络能量消耗、提高定位精度,而且能够在一定程度上防止上述 3 类攻击(即传感器攻击、反应器攻击和外来节点攻击).另外,ServLoc 通过反应器移动位置、被动接收定位请求等方法,以达到反应器节点隐匿位置的目的.

3) 在 WSAN 部署的初始阶段,反应器节点通常相对均匀地分布在网络部署区域.在完成传感器节点定位阶段后,分布的反应器才可能移动,并对某块区域的事务执行反应任务.因此在定位阶段,可以把部署区域划分成网格,部署基于位置的密钥机制进行加密认证,如文献[11,12],并利用本地反应器协调完成该网格区域内的传感器定位,从而不破坏网络的自组织性和扩展性.如图 1 所示,ServLoc 主要利用家乡方格和邻居方格内的反应器作为锚节点,协同定位家乡方格内的未知传感器节点.由于传感器节点定位完成后,反应器可以大范围地移动执行反应任务,因此,ServLoc 不影响反应器的移动性和位置的隐匿性.

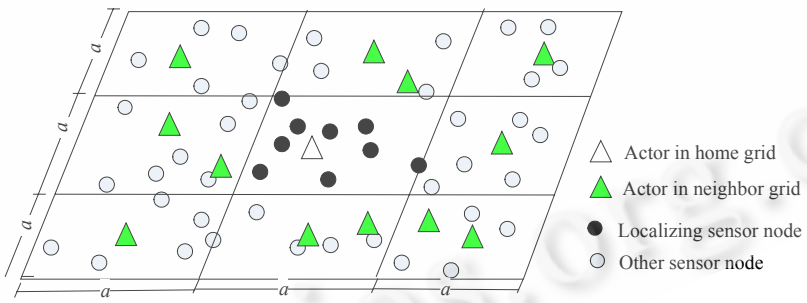

Fig.1 Localizing sensor nodes in home grid by neighbor/home actors

图 1 反应器定位家乡格内传感器示意

2 ServLoc 协议

首先,我们把部署区域划分成一个个方格,每个方格原则上包含一个或一个以上的反应器节点.因为采用分布定位方法,我们以定位如图 1 所示的家乡格内的传感器为例.为了定位这些传感器,家乡格内的反应器和邻格内的各个反应器协调完成安全位置服务.我们采用类似DV-Hop的机制[5]进行定位,即以最短路径上的跳数与平均每跳距离相乘来估算反应器与被定位传感器节点间的距离.

在定位的第 1 阶段,为了保证位置的隐匿性,每个反应器被动地接收家乡格内传感器节点的定位请求,并对消息进行认证,记录最小跳数.由于节点随机部署,未知节点和锚节点的跳段距离不是直线距离,采用传感器节点的通信半径作为平均每跳距离,过大地估算了跳段距离.即使采用文献[13]的改进公式估算平均每跳距离,也

未考虑实际环境,如地形环境对传感器通信半径的影响.ServLoc 机制采用家乡格内反应器以传感器方式工作(例如部署前,反应器可绑定同类配置的传感器节点),实际测定到每个相邻反应器的最少跳数 $H_{A_0A_i}$,然后根据到邻居反应器间的距离 $D_{A_0A_i}$,计算得到每个方向上的平均每跳距离 $d_{A_i}=D_{A_0A_i}/H_{A_0A_i}$,以进一步减少因实际环境引起无线传播性能改变而造成的距离估算误差,提高定位精确度.最后,根据未知节点到反应器节点的最少跳数 $H_{A_iS_j}$,计算反应器节点与未知节点的距离 $D_{A_iS_j}=D_{A_i}\times H_{A_iS_j}$ (符号说明见表 1).

Table 1 Notation for ServLoc protocol

表 1 ServLoc 协议符号表

Symbol	Signification	Remark
$A_i(i=1,2,\ldots,N-1)$	Actor in neighbor grids	Triangle in Fig.1
A_0	Actor in home grids	Triangle in Fig.1
$S_j(j=1,2,\ldots,M)$	Sensor in home grid *M:* The number of sensor in one grid	Black dot in Fig.1
$H_{A_iS_j}$ ($i=0,1,\ldots,N-1$), ($j=1,2,\ldots,M$)	The minimum hop number between the actor A_i and sensor S_j	
$H_{A_0A_i}$ ($i=1,2,\ldots,N-1$)	The minimum hops number between the actor A_0 and actor A_i	Actors work as sensor mode
$D_{A_iS_j}$ ($i=0,1,\ldots,N-1$) ($j=1,2,\ldots,M$)	The evaluated distance between actor A_i 与 and sensor j	
$D_{A_0A_i}$ ($i=1,2,\ldots,N-1$)	The distance between actor A_0 and actor A_i	
d_{A_i} ($i=0,1,\ldots,N-1$)	Average distance of one hop between actor A_i and sensor S_j	d_{A_0} =Avg($d_{A_iS_j}$) or evaluation by experience
$P_i(i=0,1,\ldots,N-1)$	The position of actor A_i	
$D(P_i,p_r)$	Computing the distance between actor A_i and sensor S_j	
p_r	The unverified position of sensor node	
p	The verified position of sensor node	

在定位的第 2 阶段,为防止反应器在通信过程中被攻击者定位,邻居反应器通过安全信道发送它们的估算距离 D_{A_iS} 到家乡格内的一个反应器,并移动它们自身的位置以避免暴露节点位置(当网格划分较细时,为防止反应器的位置隐匿受到影响,反应器的移动范围可以跨越网格).家乡格内的该反应器采用极大似然法估算未知节点的位置.然后,ServLoc 定位机制排除了这些估算距离误差超过阈值的反应器参与定位,迭代提高定位精度.

在 ServLoc 的定位校验协议中,各反应器根据传感器节点声明位置 p_r,计算到该传感器节点位置的距离 $D(P_i,p_r)$,设基于 DV-Hop 估算的各反应器与该传感器距离为 $D_{A_iS_k}$,阈值为Δ,如果$|D(P_i,p_r)-D_{A_iS_k}|<\Delta$,那么,该反应器认可该声明位置 p_r.最后,通过投票表决获得大多数反应器认可的传感器位置 p_r,ServLoc 位置校验机制接受该声明位置 $p=p_r$.

2.1 ServLoc定位协议

为简化协议描述,我们以定位如图 1 所示的家乡方格内的传感器节点 S_k 为例,并假定参与定位的反应器节点为 N 个.定义 ServLoc 协议中的一些主要符号见表 1.

ServLoc 定位协议.

ServLoc: **Localizing the sensor node S_k in the home grid**.

// $nbrs(S_k)$: the neighbor sensor nodes of sensor S_k

// PBS: Public Base Station

1. $PBS\rightarrow A_0,S_k,nbrs(S_k)$: *Nonce*

//Actor-Actor authentication and coordination by secure channel

//actor work as sensor when estimating d_{A_i}

2. $A_0\rightarrow *$: $m=\{A_0,P_0,Nonce,count,MAC(A_0,P_0,Nonce)\}$,

3. A_0 move to a new position for keeping secret location

4. A_i: receive m // (i=1,…,N–1)

: compute $d_{A_i} = D_{A_0A_i} / H_{A_0A_i}$

5. S_k,$nbrs(S_k)$→*: m'={S_k or $nbrs(S_k)$,$Nonce$,$count$,$MAC(S_k$ or $nbrs(S_k)$,$Nonce)$}

6. Covert A_i: receive m' // (i=0,…,N–1)

: compute $H_{A_iS_k} = \frac{\sum_{n\in nbrs(S_k)} count_n + count_{S_k}}{|nbrs(S_k)|+1} - 0.5$

: compute $D_{A_iS_k} = d_{A_i} \times H_{A_iS_k}$

7. A_i→A_0: m''={ $D_{A_iS_k}$, P_i,MAC($D_{A_iS_k}$, P_i)},

8. A_i move to a new position

9. A_0: receive m''

: compute p_r with Maximum Likelihood Estimators

: Do {

if $|D(P_i,p_r) - D_{A_iS_k}| > \Delta$, exclude A_i for localizing

re-compute p_r

} until all $|D(P_i,p_r) - D_{A_iS_k}| < \Delta$

// N_{min} is the least number of actors for localization

: if $Count(A_i) >= N_{min}$, accept p_r;

else reject p_r

由于 DV-Hop 中计算未知节点与锚节点的跳数都是整数,但应用中最后一跳可能是不完整的一跳.因此,ServLoc 定位协议中,步骤 6 采用文献[13]建议的公式估算最小跳数 $H_{A_iS_k}$.实际上,如果反应器能够通过 RSSI 等手段估算最后一跳的分数值,可以更加精确地估算距离值.

2.2 ServLoc位置校验协议

位置校验的方法可采用家乡方格内的反应器单独校验传感器位置,但是容易遭受第 1.1 节中提到的各类攻击,即使未收到攻击,由于误差等问题,校验机制仍可能拒绝传感器节点的位置报告.为了减少各类攻击的成功概率和误检率,ServLoc 采用本地相邻反应器参与,投票表决校验传感器的位置报告.

ServLoc 校验协议.

Voting-Based location verification with hidden actors.

1. PBS→S_k: $Nonce$

2. S_k→*: m={p_r,$count$,$MAC(p_r$,$Nonce)$}

3. Covert A_i: receive m

: compute $H_{A_iS_k}$

: compute $D_{A_iS_k} = d_{A_iS_k} \times H_{A_iS_k}$

: if $|D(P_i,p_r) - D_{A_iS_k}| < \Delta$

A_i→*: m'={A_i,S_k,$accept\ p_r$,$Nonce$,$MAC(A_i$,S_k,$accept\ p_r$,$Nonce)$}

else

A_i→*: m'={A_i,S_k,$reject\ p_r$,$Nonce$,$MAC(A_i$,S_k,$reject\ p_r$,$Nonce)$}

4. A_i move to a new position

5. Covert A_i: receive m'

// N_{min} is the least number of actor for accepting p_r

: if $count(accepted\ p_r) >= N_{min}$

Accept $p=p_r$

else reject p_r

3 安全分析

3.1 鲁棒性

针对 ServLoc 协议进行位置攻击可分为两类:

第 1 类攻击是篡改 ServLoc 定位或校验机制中反应器与传感器之间的距离,从而影响定位精度或定位校验协议的有效性.例如,传感器攻击:被捕获的传感器节点通过增加或减少跳数计数器值来攻击反应器与传感器之间的距离测量;蠕虫洞攻击:该攻击通过攻击者合作,把消息包从一个地方经过隧道在另一个地方进行回放攻击,这样,最短路径可能被篡改,个别反应器与传感器之间的距离被改变;反应器攻击:在定位机制中,被捕获的反应器可能直接篡改它到被定位传感器节点的距离;在校验机制中,被捕获的反应器可能直接拒绝传感器报告的真实位置;外来节点攻击:外来节点通过阻塞某个区域,从而改变最短路径,达到改变反应器与传感器距离值的目的.但是,由于这些攻击只能篡改一对或少数几对传感器与反应器节点间的距离值,这些虚假的参考距离将被 ServLoc 定位协议过滤(见 ServLoc 定位协议步骤 9).在 ServLoc 定位协议中,N 个参考距离中只要有 $N_{\min}$ 个未被篡改,则 ServLoc 仍旧能安全定位,因此,ServLoc 定位协议在一定程度上能够容忍入侵.而且,即使攻击者在定位阶段欺骗成功,ServLoc 位置校验机制仍将发现它们的位置欺骗,从而通过表决拒绝接受该错误位置信息.

第 2 类攻击是传感器节点宣布自己的虚假位置或最后反应器通知未知传感器节点错误位置信息.但是,如果校验反应器被捕获的数量少于 $N-N_{\min}$,ServLoc 校验机制仍将检测出这些攻击,从而拒绝该虚假位置信息.因为校验反应器的位置是隐匿的,并且可以移动.因此,第 2 类攻击欺骗校验协议成功,从而接受它们的虚假位置概率很小,第 3.3 节将详细加以讨论.

3.2 节点位置隐匿

反应器:由于反应器被动接收传感器定位信息,测量平均每跳距离时的工作方式与传感器定位请求一样,因此,攻击者很难辨别反应器信号并通过信号检测对反应器进行逆向定位或猜测反应器位置.另外,反应器通过安全通道相互通信,定位协议中,反应器宣布自身位置、最后通知传感器节点位置或校验协议中宣布接收/拒绝传感器位置后,立刻移动位置并隐匿,使得攻击者必须以较大代价才能对反应器进行定位攻击.

传感器:ServLoc 中传感器节点无法对本地反应器(如图 1 所示的反应器节点)进行位置隐匿,但是可以通过设定定位请求包广播的最多跳数来实现对图 1 网格外的节点进行位置隐匿.如要对本地的其他传感器节点隐匿自己的位置,ServLoc 协议中传感器与反应器通信前建立会话密钥并加密位置信息,以增加攻击者的攻击代价.

3.3 ServLoc校验机制的灵敏度

在 ServLoc 校验机制中,如果设置阈值Δ=0,假阴性率(位置欺骗成功概率)为 0,但是,由于锚节点位置误差和定位机制第 1 阶段的距离估算误差,假阳性率(校验机制拒绝传感器节点正确报告位置的概率)为 1.如果设置 $\Delta=\frac{3\sqrt{2}}{2}a$,则攻击者总能攻击成功,即假阴性率为 1.因此,需要确定一个合适的阈值Δ,以平衡位置校验机制的假阳性率和假阴性率.

在 ServLoc 校验机制中,有两类误差将影响校验机制的假阳性率:一类是锚节点本身的位置误差 $error_p$;另一类是估算反应器与传感器间的距离误差 $error_d$.我们假设这些误差服从高斯分布 $error_p\sim N(0,\sigma_p^2)$和 $error_d\sim N(0,\sigma_d^2)$,并设$\Delta=k\sigma$.其中,$k$ 是一个正实数.对独立高斯分布来说,标正偏差 $\sigma=\sqrt{\sigma_p+\sigma_d}$.当一个反应器单独校验传感器位置时,假阳性率为

$$P_{rFP}=1-Pr(|D(P_i,p)-D_{A_iS_j}|<\Delta)=1-Pr(-k\sigma<D(P_i,p)-D_{A_iS_j}<k\sigma)=1-\frac{2}{\sqrt{\pi}}\int_0^{\frac{k}{\sqrt{2}}}e^{-u^2}du=1-erf\left(\frac{k}{\sqrt{2}}\right).$$

在 ServLoc 校验协议中,N 个反应器(通常 $N\geq 9$)校验一个传感器的位置.当至少 $N_{\min}$ 个反应器接受该位置

时,ServLoc 位置校验机制接受该位置信息.因此,以参与定位的反应器数目 N=9 为例,ServLoc 校验协议拒绝接受传感器节点正确报告位置的概率(假阳性率) P_{rFP}^m 为

$$P_{rFP}^m = 1 - \sum_{i=m}^{9} C_9^i \left[erf\left(\frac{k}{\sqrt{2}}\right)\right]^i \left[1 - erf\left(\frac{k}{\sqrt{2}}\right)\right]^{9-i} \tag{1}$$

另外,在 ServLoc 校验协议中,位置欺骗攻击成功的最大概率(假阴性率) $P\max_D^m$ 为

$$P\max_D^m = \frac{2\pi k\sigma}{a} \sum_{i=m-1}^{8} C_8^i \left(\frac{2.93k\sigma}{a}\right)^i \left(1 - \frac{2.93k\sigma}{a}\right)^{8-i} + \left(1 - \frac{2\pi k\sigma}{a}\right) \sum_{i=m}^{9} C_9^i \left(\frac{2.93k\sigma}{a}\right)^i \left(1 - \frac{2.93k\sigma}{a}\right)^{9-i} \tag{2}$$

其中,a 是方格的边长.

公式(2)的证明:

前提:每个校验反应器在家乡方格和邻居方格内为均匀概率分布,位置隐匿;待校验的传感器节点必须在家乡方格内;攻击者能够任意篡改待校验的位置信息,任意篡改校验反应器与待校验传感器的距离,以便通过 ServLoc 校验机制.

通过实验,当Δ<<a 时,攻击者欺骗性宣布(或通过篡改)待校验的位置为家乡方格中心;并猜测隐匿的校验反应器在如图 2 所示的圆环或圆环片断内;此时,攻击者攻击 ServLoc 位置校验机制的成功概率(假阴性率)达到最大 $P\max_D^m$.分两种情况讨论:

1) 攻击者欺骗家乡方格内校验反应器成功的最大成功概率为 $P\max_1$:攻击者宣称待校验的传感器位置在方格中心,猜测该隐匿反应器在内径为 $r=a/2-\Delta$上,外径为 $r=a/2+\Delta$的圆环内(如图 2 所示),此猜测成功的概率即为 $P\max_1$.

$$P\max_1 = \frac{S_{ring}}{S_{grid}} \approx \frac{2\pi\frac{a}{2}2\Delta}{a^2} = \frac{2\pi k\sigma}{a}.\text{其中,}\Delta<<a.$$

2) 攻击者欺骗邻居方格内校验反应器成功的最大概率为 $P\max_2$,又分两种情况:

2-1) 针对对角方格内的反应器:圆环片断内径为 $r_{11}=\frac{\sqrt{10}}{2}a-\Delta$,外径 $r_{12}=\frac{\sqrt{10}}{2}a+\Delta$,角度$\theta_1$=2argtan(1/2)(如图 2 所示).此时,

$$P\max_{2\text{-}1} \approx \frac{S_{ringsec}}{S_{grid}} \frac{2\arctan\left(\frac{1}{2}\right)\frac{\sqrt{10}}{2}a \times 2\Delta}{a^2} = \frac{2.93k\sigma}{a}.\text{其中,}\Delta<<a.$$

2-2) 针对其他邻居方格内的反应器:圆环片断内径为 $r_{21}=\frac{3}{2}a-\Delta$,外径 $r_{22}=\frac{3}{2}a+\Delta$,角度$\theta_2$=2argtan(1/3)(如图 2 所示).此时,

$$P\max_{2\text{-}2} \approx \frac{S_{ringsec}}{S_{grid}} \frac{2\arctan\left(\frac{1}{3}\right)\frac{3}{2}a \times 2\Delta}{a^2} = \frac{1.93k\sigma}{a}.\text{其中,}\Delta<<a.$$

为简化分析,设 $P\max_2=\max(P\max_{2\text{-}1}, P\max_{2\text{-}2})$,则 $P\max_2=\frac{2.93k\sigma}{a}$.

在 ServLoc 校验机制中,攻击者攻击成功的概率 $P\max_D^m$ 是成功欺骗至少 $N_{\min}$ 个校验反应器.

当家乡格反应器被欺骗成功时,攻击成功最大概率为 $P\max_{D_1}^m = P\max_1 \sum_{i=m-1}^{8} C_8^i (P\max_2)^i (1-P\max_2)^{8-i}$,

否则, $P\max_{D_2}^m = (1-P\max_1) \sum_{i=m}^{9} C_9^i (P\max_2)^i (1-P\max_2)^{9-i}$,

因此, $P\max_D^m = P\max_{D_1}^m + P\max_{D_2}^m$,

$$P\max_D^m = P\max_1 \sum_{i=m-1}^{8} C_8^i (P\max_2)^i (1-P\max_2)^{8-i} + (1-P\max_1)\sum_{i=m}^{9} C_9^i (P\max_2)^i (1-P\max_2)^{9-i},$$

$$P\max_D^m = \frac{2\pi k\sigma}{a}\sum_{i=m-1}^{8} C_8^i \left(\frac{2.93k\sigma}{a}\right)^i \left(1-\frac{2.93k\sigma}{a}\right)^{8-i} + \left(1-\frac{2\pi k\sigma}{a}\right)\sum_{i=m}^{9} C_9^i \left(\frac{2.93k\sigma}{a}\right)^i \left(1-\frac{2.93k\sigma}{a}\right)^{9-i}.$$

得证. □

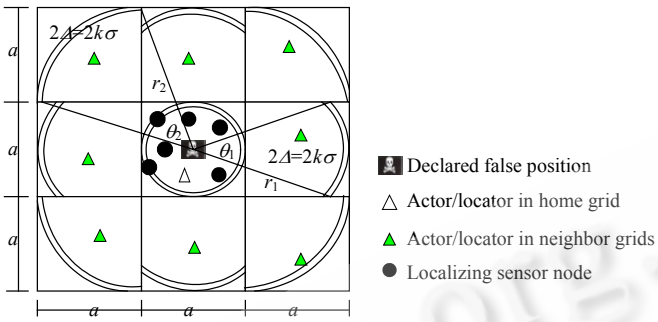

Fig.2 The attacker guess the verifying actors in the ring or ring sections and disguise itself in the center of home grid by tempering distance between sensor node and actor node to maximize probability of successful attack in verification scheme of ServLoc

图 2 攻击者先猜测校验反应器在圆环或扇形环内,并通过修改传感器和反应器节点间的距离以伪装自己在家乡网格中心.此时,攻击者躲避 ServLoc 位置校验机制从而攻击成功的概率最大

攻击者假设各隐匿的校验反应器在圆环/圆环片断内;欺骗校验协议传感器节点位置在家乡方格中心,并成功篡改各参考距离.

在实验中,我们设置方格的边长 a=300,传感器通信半径 r=30,位置和距离误差的标准偏差 σ=3,ServLoc 校验协议中,$N_{\min}$=5,7,9.图 3 显示了 ServLoc 校验协议中,最大攻击成功概率(假阴性) $P\max_D^m$、拒绝正确位置报告信息的误检率(假阳性) P_{rFP}^m 与敏感度 s 的关系(敏感度 s=1/k,阈值 $\Delta=k\sigma$,σ为位置和距离误差的标准偏差).其中,s 与期望误差(阈值)Δ($\Delta=k\sigma$)成反比.当 $s\to\infty$时,ServLoc 校验协议非常敏感,不能容忍任何反应器的位置误差和协议中的距离估算误差;当 $s\to 0$ 时,ServLoc 校验协议将容忍一切误差.

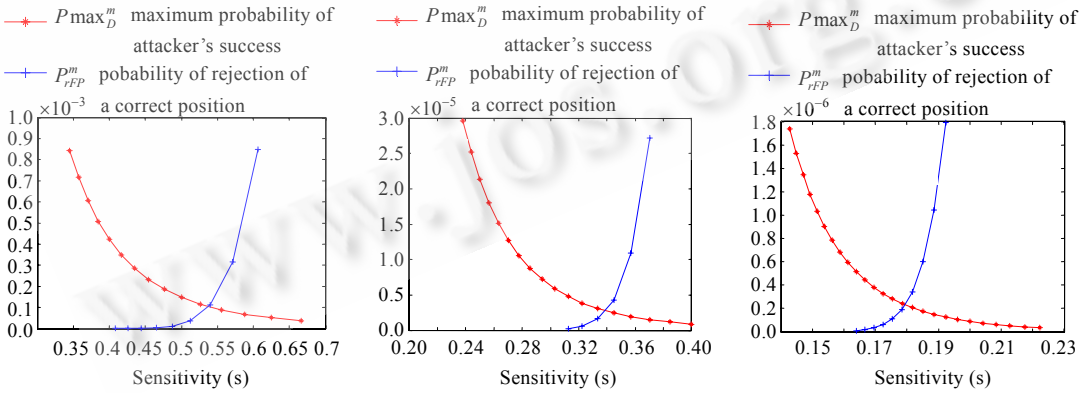

Fig.3 The frequency of false positives and false negatives

图 3 假阴性率、假阳性率与敏感度 s 的关系

图 3(a)显示,当至少 5 个校验反应器接受待校验位置时($N_{\min}$=5),ServLoc 校验机制将接受该待校验的位置.在曲线交叉点,s=0.54, $P\max_D^m = P_{rFP}^m$ =1.2×10^{-4}.类似地,图 3(b)表示 $N_{\min}$=7 时,交叉点值为 s=0.34, $P\max_D^m = P_{rFP}^m$ = 3×10^{-6}.图 3(c)表示 $N_{\min}$=9 时,交叉点值为 s=0.18, $P\max_D^m = P_{rFP}^m$ =2.2×10^{-7}.交叉点值在一定程度上反映了 ServLoc 校验机制的性能.实验表明,当 $N_{\min}$ 值提高时,ServLoc 校验协议敏感度 s 降低,假阴性率 $P\max_D^m$ 和假阳性率 P_{rFP}^m 均可有效下降,ServLoc 校验机制的性能得到有效改善.另外,随着反应锚节点位置误差和距离估算误差的标准偏差σ的减少,假阴性率和假阳性率也将随之降低,ServLoc 校验机制的性能得到进一步的提高.

4 讨 论

在传感器攻击、反应器攻击和外来节点攻击中,反应器攻击对 ServLoc 协议最具威胁性,下面将主要对反应器攻击和防御方法进行讨论.

在 ServLoc 定位协议中,A_0(家乡方格内的反应器)收集到所有的参考距离信息后,对家乡方格内的传感器节点进行定位.实际应用中,A_0 可能是潜在的攻击者,这样,它所在方格内的所有传感器节点将可能无法定位或错误定位.解决方法是,邻居反应器都协作参与定位计算,并与 A_0 宣布的位置进行比较.当结果不一致时,启用入侵检测响应系统清除 A_0 和其他入侵节点,再选择可信邻居反应器(或基站)对家乡方格内的传感器节点重新计算定位.关于入侵检测响应模型,我们在文献[14]中已有阐述,这里不再赘述.

另外,在 ServLoc 定位和位置校验协议中假设网络初始化部署阶段(也即定位阶段)时,即使在局部区域,攻击者也不能捕获大多数反应器节点并破解密钥,使得它们成为潜在的攻击节点;但当该假设不成立时(即局部区域的反应器在初始化阶段大多数转化为攻击节点),这些反应器的联合攻击将可能导致该局部区域的传感器节点定位和位置校验失效.一种解决方法是,在 ServLoc 协议中引入更大范围内更多的反应器(例如非邻居方格内的反应器)参与对家乡方格内的传感器节点定位,这样使得攻击者在大范围区域内捕获大多数反应器的难度提高,从而降低了局部区域内传感器节点定位失效的概率.但是,这种解决方案使得传感器节点的定位请求包需要广播更大的范围,从而增加了网络的通信和能量消耗.另一种解决方法是,当局部区域内的反应器节点对定位结果不一致时,采用基于时间约束和拓扑一致性检测的方法.当每个中间节点转发定位请求报文时,记录仿篡改的身份 ID 和时间戳,同时要求反应器把收到的定位请求包和反应器自身位置作为证据转发给基站,以此来防止反应器篡改参考距离或使得基站根据节点拓扑关系能够比较容易地检测出这些企图篡改参考距离的反应器节点.由于这些通信计算主要在反应器节点和基站之间进行,因此可在一定程度上平衡网络能量消耗和通信开销.但防止节点的联合攻击是一个极其有挑战性的问题,除了采取防御机制提高攻击代价以外,还需引入入侵检测响应系统来解决此类攻击.

5 结 论

本文主要分析了无线传感反应网络(WSAN)中位置服务机制可能遭受的各类攻击,并提出了一种适合 WSAN 的安全定位协议、位置校验协议、重要节点隐匿机制和安全位置报告.通过消息码认证,ServLoc 能够有效地防御这些通过篡改消息包内容进行位置攻击的外部攻击.由于 ServLoc 定位协议能够过滤虚假定位信息,ServLoc 定位校验协议采用投票表决的方式校验传感器节点的位置信息.因此,即使在遭受一定强度的位置攻击的情况下,ServLoc 仍能进行安全位置服务.通过被动接收定位请求和反应器移动位置,ServLoc 能够保持重要节点位置的隐匿性.另外,利用 WSAN 的异构特性,ServLoc 机制利用反应器作为定位锚节点并进行定位计算,节省了传感器节点的能量和网络部署成本.

致谢 在此,我们要感谢匿名审稿人细致而认真地审阅本文,并指出本文的一些笔误、值得探讨的问题和有益的建议.

References:

[1] Akyildiz IF, Kasimoglu IH. Wireless sensor and actor networks: Research challenges. Ad Hoc Networks, 2004,2(4):351−367.

[2] Sun LM, Li JZ, Chen Y, Zhu HS. Wireless Sensor Network. Beijing: Tsinghua University Press, 2005 (in Chinese).

[3] Bahl P, Padmanabhan VN. RADAR: An in-building rf-based user location and tracking system. IEEE Infocom, 2000. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=832252

[4] Savvides A, Han C, Srivastava M. Dynamic fine-grained localization in ad-hoc networks of sensors. In: Proc. of the ACM MobiCom 2001. 2001. 166−179. http://portal.acm.org/citation.cfm?id=381693

[5] Bulusu N, Heidemann J, Estrin D. GPS-Less low cost outdoor localization for very small devices. IEEE Personal Communications Magazine, 2000,7(5):28−34.

[6] Wang FB, Shi L, Ren FY. Self-Localization systems and algorithms for wireless sensor networks. Journal of Software, 2005,16(5): 857−868 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/16/857.htm

[7] Liu D, Ning P, Du W. Attack-Resistant location estimation in sensor networks. In: Proc. of the Int'l Conf. on Information Processing in Sensor Networks (IPSN). 2005. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1440904

[8] Li Z, Trappe W, Zhang Y, Nath B. Robust statistical methods for securing wireless localization in sensor networks. In: Proc. of the Int'l Conf. on Information Processing in Sensor Networks (IPSN). 2005. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1440903

[9] Capkun S, Cagalj M, Srivastava M. Securing localization with hidden and mobile base stations. In: Proc. of the IEEE INFOCOM 2006. 2006. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4146955

[10] Lazos L, Poovendran R. ServLoc: Robust localization for wireless sensor networks. ACM Trans. on Sensor Networks, 2005,1(1): 73−100.

[11] Du WL, Wang RH, Ning P. An efficient scheme for authenticating public keys in sensor networks. In: Proc. of the 6th ACM Int'l Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc). 2005. http://portal.acm.org/citation.cfm?id=1062689.1062698

[12] Merkle R. Secrecy, authentication, and public key systems [Ph.D. Thesis]. Stanford: Stanford University, 1979.

[13] Nagpal R, Shrobe H, Bachrach J. Organizing a global coordinate system from local information on an ad hoc sensor network. In: Proc. of the IPSN 2003. New York: Springer-Verlag, 2003. 151−152.

[14] Ma JQ, Zhang SY, Zhong YP, Tong XW. SAID: A self-adaptive intrusion detection system in wireless sensor networks. In: Proc. of the WISA 2006. LNCS 4298, 2007. 60−73. http://www.springerlink.com/index/h661852714r33882.pdf

附中文参考文献:

[2] 孙利民,李建中,陈渝,朱红松.无线传感器网络.北京:清华大学出版社,2005.

[6] 王福豹,史龙,任丰原.无线传感器网络中的自身定位系统和算法.软件学报,2005,16(5):857−868. http://www.jos.org.cn/1000-9825/16/857.htm

马建庆(1974－),男,浙江绍兴人,博士,主要研究领域为无线通信与网络,移动计算,安全.

张世永(1950－),男,教授,博士生导师,CCF高级会员,主要研究领域为计算机网络的应用和安全,数据通信.

钟亦平(1953－),女,教授,主要研究领域为网络安全,协议分析与测试.